NATHAN R. RING
NEVADA STATE BAR NO. 12078
STRANCH , JENNINGS & GARVEY, PLLC
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
Telephone: (725) 235-9750
lasvegas@stranchlaw.com

CARL V. MALMSTROM
(*pro hac vice forthcoming*)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. JACKSON BLVD., SUITE 1700
CHICAGO, IL 60604
Telephone: (312) 984-0000
Facsimile: (212) 686-0114
malmstrom@whafh.com

RACHELE R. BYRD
(*pro hac vice forthcoming*)
ALEX J. TRAMONTANO
(*pro hac vice forthcoming*)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com
tramontano@whafh.com

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

BRIDGET O'NEILL and KIRK MOSES, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

PERRY JOHNSON & ASSOCIATES, INC. and COUNTY OF COOK, ILLINOIS,

Defendants.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

I. INTRODUCTION

1. Plaintiffs Bridget O'Neill and Kirk Moses ("Plaintiffs") bring this class action in this Court against Defendants Perry Johnson & Associates, Inc. ("PJ&A") and the County of Cook, Illinois ("Cook County" and, collectively, "Defendants") for their failure to prevent a cyberattack that resulted in the theft and dissemination (the "Data Breach") of Plaintiffs' and approximately 8.9 million other similarly situated individuals' sensitive information,[1] including, upon information and belief, their personally identifying information ("PII") and personal health information ("PHI"), including names, dates of birth, addresses, medical record numbers, hospital account numbers, admission diagnoses, dates and times of service, Social Security numbers, insurance information, clinical information such as laboratory and diagnostic testing results, medications, treatment facility names, and healthcare provider names (collectively, "Personally identifiable information" or "PII"). [2, 3]

2. Between approximately March 27, 2023, and May 2, 2023, an unauthorized third-party gained access to PJ&A's network system and obtained files containing information about Cook County's current and former patients.

3. Defendant PJ&A provides transcription services to healthcare organizations and physicians for dictating and transcribing patient notes for hospital groups nationwide.

4. Defendant Cook County is an incorporated county in the U.S. state of Illinois.

5. Cook County Health ("CCH") is an integrated healthcare network, and a part of Cook County, and provides care to more than 500,000 individuals through the health system and the health plan.

6. Upon information and belief, individuals, including Plaintiffs and Class members, who were consumers of Defendants' healthcare services and transcription services, and are

---

[1] *See* U.S. Department of Health and Human Services Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, last accessed November 22, 2023.

[2] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[3] *See* https://www.hipaajournal.com/pja-data-breach/, last accessed November 21, 2023.

required to entrust Defendants with sensitive, non-public PII and PHI, without which Defendants could not perform their regular business activities, in order to obtain healthcare products and/or services from Defendants. Defendants retain this information for many years and even after the consumer relationship has ended.

7. By obtaining, collecting, using, and deriving a benefit from the PII and PHI of Plaintiffs and Class members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

8. Defendants failed to adequately protect Plaintiffs' and Class members' PII and PHI—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII and PHI was compromised due to Defendants' negligent and/or careless acts and omissions and its utter failure to protect consumers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class members' PII and PHI because of its value in exploiting and stealing the identities of Plaintiffs and Class members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. Plaintiffs bring this action on behalf of all persons whose PII and PHI was compromised as a result of Defendants' failure to: (i) adequately protect the PII and PHI of Plaintiffs and Class members; (ii) warn Plaintiffs and Class members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII and PHI using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts at least to negligence and violates federal and state statutes.

10. Defendants disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII and PHI of Plaintiffs and Class members was compromised through disclosure to an unknown and unauthorized third party.

11. Plaintiffs and Class members have a continuing interest in ensuring that their

information is and remains safe, and they should be entitled to injunctive and other equitable relief.

12. Plaintiffs and Class members have suffered injury as a result of Defendants' conduct. These injuries include: (i) invasion of privacy; (ii) theft of PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

13. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendants' inadequate data security practices.

II. PARTIES

14. Plaintiff Bridget O'Neill is, and at all times relevant, has been a citizen of Illinois residing in Cook County. Plaintiff O'Neill obtained healthcare or related services from Cook County through CCH. As a condition of receiving services, Defendants required Plaintiff O'Neill to provide them with her PII/PHI.

15. Plaintiff Kirk Moses is, and at all times relevant, has been a citizen of Chicago, IL. Plaintiff Moses obtained healthcare or related services from Cook County through CCH. As a condition of receiving services, Defendants required Plaintiff Moses to provide them with his PII/PHI.

16. Defendant Perry Johnson & Associates is a Nevada corporation with its principal place of business at 1489 W Warm Springs Rd., Henderson, NV 89014. Its registered agent for service is C T Corporation System, 701 S. Carson St., Suite 200, Carson City, NV 89701.

17. Defendant Cook County is an incorporated county in the U.S. state of Illinois.

III. JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class member is a citizen of a state different from Defendant.

19. This Court has jurisdiction over Defendant because it operates in this District. Defendant Perry Johnson & Associates, Inc. is a corporation incorporated under the laws of Nevada, has its principal place of business in Nevada, and does significant business in Nevada.

20. This Court has personal jurisdiction over Defendant Cook County, because it transacts business within this state and makes or performs contracts within this state by doing business with PJ&A.

21. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because PJA has its principal place of business in Nevada, and a substantial part of the events giving rise to Plaintiffs' claims arose in this District.

IV. FACTUAL ALLEGATIONS

A. *Defendants' Respective Businesses*

22. Defendant PJ&A "provides medical transcription services to various healthcare qorganizations."[4]

23. Defendants Cook County and CCH used PJ&A for medical transcription and dictation services.[5]

24. Plaintiffs and Class members are current or former patients of Cook County and CCH who entrusted PJ&A with their PII/PHI.

25. As a necessary part of its regular business activities, Defendants collected and

[4] Cyber Incident Notice, PERRY JOHNSON & ASSOCS., https://www.pjats.com/downloads/Notice.pdf (last accessed Nov. 21, 2023) (hereinafter "PJA Notice").

[5] Notice of Data Security Incident, COOK COUNTY, https://cookcountyhealth.org/compliance-notice/ (last accessed Nov. 21, 2023).

stored the PII of Plaintiffs and Class members.

26. As a condition of receiving its products and/or services, Defendants require that patients, including Plaintiffs and Class members, entrust it with highly sensitive personal information.

27. The information held by Defendants in their computer systems at the time of the Data Breach included the unencrypted PII of Plaintiffs and Class members.

28. Upon information and belief, Defendants made promises and representations to its patients, including Plaintiffs and Class members, that the PII and PHI collected from them would be kept safe and confidential, that the privacy of that information would be maintained, and that Defendants would delete any sensitive information after it was no longer required to maintain it.

29. Indeed, Defendant Cook County's Privacy Policy provides: "We are required by law to protect the privacy of your health information and to provide you with this information and if you are affected, to notify you following a breach of unsecured protected health information. State and federal privacy laws strengthen our commitment to you, as our patient, to carefully maintain your confidentiality."[6]

30. Plaintiffs and Class members provided their PII to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

31. Plaintiffs and the Class members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class members relied on the sophistication of Defendants to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class members value the confidentiality of their PII and demand security to safeguard their PII.

32. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class members from involuntary disclosure to third parties. Defendants have a legal duty to

[6] *See* https://cookcountyhealth.org/wp-content/uploads/2019_01.01.50-Notice-of-Privacy-Practices-English.pdf (last visited Nov. 22, 2023).

keep patients' PII and PHI safe and confidential.

33. Defendants had obligations created by the FTC Act, contract, industry standards, and representations made to Plaintiffs and Class members, to keep their PII and PHI confidential and to protect it from unauthorized access and disclosure.

34. Defendants derived a substantial economic benefit from collecting Plaintiffs' and Class members' PII and PHI. Without the required submission of PII and PHI, Defendant could not perform the services it provides.

35. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' PII and PHI, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class members' PII and PHI from disclosure.

B. *The Data Breach*

36. Between approximately March 27, 2023, and May 2, 2023, "An unauthorized party gained access to the PJ&A network . . . and, during that time, acquired copies of certain files from PJ&A systems."[7]

37. Despite learning of the Data Breach on or about May 2, 2023 and determining that PII and PHI was involved in the breach, Defendant PJ&A did not begin sending notices of the Data Breach (the "Notice of Data Breach Letter") until late October or early November 2023.[8]

38. According to the Notice of Data Security Incident posted on PJ&A's website, the PII/PHI affected in the Data Breach included names, dates of birth, addresses, medical record numbers, hospital account numbers, admission diagnoses, dates and times of service, Social Security numbers, insurance information, clinical information such as laboratory and diagnostic testing results, medications, treatment facility names, and healthcare provider names. [9]

39. CCH notified 1.2 million patients that their medical records had been breached in the PJ&A incident. The exact number of the people affected by this cyber-incident had remained unknown until PJ&A submitted the relevant information to the breach portal of the U.S.

---

[7] PJA Notice, supra note 9.
[8] *Id.*
[9] *Id.*

Department of Health and Human Services Office for Civil Rights, which now confirms the number to be 8,952,212 patients.[10] Plaintiff Moses received a copy of the CCH notice dated November 7, 2023.[11] Plaintiff O'Neill received a copy of the CCH notice dated November 7, 2023.[12]

40. A ransomware attack, like that experienced by Defendants is a type of cyberattack that is frequently used to target companies due to the sensitive data they maintain.[13] In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[14]

41. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[15] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence [….] [T]he initial assumption should be that data may have been exfiltrated."[16]

42. An increasingly prevalent form of ransomware attack is the encryption+exfiltration attack in which the attacker encrypts a network and exfiltrates the data contained within. In the third quarter of 2020, "[a]lmost 50% of ransomware cases included the

---

[10] See U.S. Department of Health and Human Services Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, last accessed November 22, 2023.

[11] See Exhibit A, "Notice of Data Security Incident" sent by Cook County Health dated November 7, 2023.

[12] *Id.*

[13] ZDNET.com, *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at: https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/ (last visited Oct. 2, 2023).

[14] Center for Internet Security, *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at: https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (last visited Oct. 2, 2023).

[15] *Id.*

[16] Financial Post, *Threat group posts files allegedly from Canadian military college*, available at: https://financialpost.com/technology/tech-news/threat-group-posts-files-allegedly-from-canadian-military-college (last accessed Oct. 2, 2023).

threat to release exfiltrated data along with encrypted data."[17] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[18] And even where companies pay for the return of data, attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[19]

43. Despite these warnings, Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class members, allowing the attackers free access to the PII and PHI stored therein. Defendants failed to properly verify the credentials of the attacker and failed to have in place systems to prevent and detect the ransomware attack.

44. The attacker accessed and acquired information from Defendants' files, which on information and belief, contained unencrypted PII and PHI of Plaintiffs and Class members, including their Social Security numbers and other sensitive information. Plaintiffs' and Class members' PII and PHI was accessed and stolen in the Data Breach.

45. Plaintiffs further believe their PII and PHI, and that of Class members has been or will be sold on the dark web, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

C. *Defendants Acquire, Collect, and Store Plaintiffs' and Class Members' PII and PHI*

46. Defendants collected, retained, and stored the PII and PHI of Plaintiffs and Class members and derived a substantial economic benefit from that PII and PHI. But for the collection of Plaintiffs' and Class members' PII and PHI, Defendants would be unable to perform their services.

47. By obtaining, collecting, and storing the PII and PHI of Plaintiffs and Class members, Defendants assumed legal and equitable duties and knew or should have known that it

---

[17] Coveware.com, *Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues*, https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report (last accessed Oct. 2, 2023).

[18] *Id.*

[19] *Id.*

was responsible for protecting the PII and PHI from disclosure.

48. Plaintiffs and Class members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

49. Defendants could have prevented this Data Breach by properly securing its network and encrypting the files and file servers containing the PII and PHI of Plaintiffs and Class members.

50. Defendants made promises to Plaintiffs and Class members to safely maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

D. *Defendants Knew or Should Have Known of the Risk Because Institutions in Possession of PII and PHI Are Particularly Susceptible to Cyber Attacks*

51. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store PII and PHI, like Defendants, preceding the date of the breach.

52. Data thieves regularly target companies like Defendants due to the highly sensitive information in their custody. Defendants knew and understood that unprotected PII and PHI is valuable and highly sought after by criminals who seek to illegally monetize that PII and PHI through unauthorized access.

53. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[20]

54. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII and PHI that it collected

[20] Identity Theft Resource Center, *2021 Data Breach Report*, available at: https://www.idtheftcenter.org/wp-content/uploads/2022/04/ITRC_2021_Data_Breach_Report.pdf (last visited Oct. 2, 2023).

and maintained would be targeted by cybercriminals.

55. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class members from being compromised.

56. Moreover, Defendants were, or should have been, aware of the foreseeable risk of a cyberattack, like the one it experienced.

57. Accordingly, Defendants knew, or should have known, the importance of safeguarding the PII and PHI entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class members as a result of a breach.

58. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' server(s), amounting to, upon information and belief, potentially millions of individuals' detailed PII/PHI and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

59. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiffs and Class members.

60. The ramifications of Defendants' failure to keep secure the PII and PHI of Plaintiffs and Class members are long lasting and severe. Once PII/PHI is stolen, fraudulent use of that information and damage to victims may continue for years.

E. ***Value of Personally Identifiable Information***

61. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[21] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number,

[21] 17 C.F.R. § 248.201 (2013).

employer or taxpayer identification number."[22]

62. The PII and PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[23]

63. For example, PII can be sold at a price ranging from $40 to $200.[24] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[25]

64. Moreover, Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[26]

65. Regarding PHI, all-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to

---

[22] *Id*.

[23] Digital Trends, *Your personal data is for sale on the dark web. Here's how much it costs* (Oct. 16, 2019), available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 2, 2023).

[24] Experian, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, available at: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 2, 2023).

[25] VPNOverview, *In the Dark*, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visitied Oct. 2, 2023).

[26] Social Security Administration, *Identity Theft and Your Social Security Number* (July 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 2, 2023).

$1,300 each on the black market.[27] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[28]

66. Based on the foregoing, the information at issue in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

67. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[29]

68. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

69. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting

---

[27] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[28] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[29] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 2, 2023).

from data breaches cannot necessarily rule out all future harm.[30]

F. *Defendants Failed to Comply with FTC Guidelines*

70. Federal and State governments have likewise established security standards and issued recommendations to prevent and limit the impact of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[31] Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an 'unfair practice' in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See*, *e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

71. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[32] The guidelines note businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

72. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex

---

[30] Report to Congressional Requesters, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf ("GAO Report") (last visited Oct. 2, 2023).

[31] Federal Trade Commission, *Start With Security: A Guide for Business*, *available at*: https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited Oct. 2, 2023).

[32] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, *available at*: https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Oct. 2, 2023).

passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

73. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

74. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class members' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

75. Defendants were at all times fully aware of its obligation to protect the personal and financial data of Plaintiffs and Class members. Defendants were also aware of the significant repercussions when it failed to do so.

G. *Defendants Failed to Comply with Industry Standards*

76. As noted above, experts studying cybersecurity routinely identify entertainment companies as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

77. Some industry best practices that should be implemented by Health Care Systems and Medical Transcription companies dealing with sensitive PII and PHI, like Defendants, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

78. Other best cybersecurity practices that are standard in the entertainment industry

include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

79. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness. Defendants failed to comply with these accepted standards in the entertainment industry, thereby permitting the Data Breach to occur.

H. *Defendants Breached Their Duty to Safeguard Plaintiffs' and Class Members' PII/PHI*

80. In addition to its obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Class members.

81. Had Defendants remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class members' confidential PII and PHI.

I. *Common Injuries and Damages*

82. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII and PHI ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class members has materialized and is

present and continuing, and Plaintiffs and Class members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; (e) invasion of privacy; and (f) the continued risk to their PII and PHI, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' PII and PHI.

J. ***The Data Breach Increases Victims' Risk of Identity Theft***

83. Plaintiffs and Class members are at a heightened risk of identity theft for years to come.

84. The unencrypted PII and PHI of Plaintiffs and Class members will end up for sale on the dark web because that is the modus operandi of hackers. In addition, unencrypted PII and PHI may fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of Plaintiffs and Class members. Unauthorized individuals can easily access the PII and PHI of Plaintiffs and Class members.

85. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII and PHI to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

86. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

87. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information

through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

88. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[33]

89. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

90. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

91. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiffs and the other Class members.

92. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

---

[33] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecurity.com/tag/fullz/ (last visited Oct. 2, 2023).

93. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

K. *Loss Of Time to Mitigate Risk of Identity Theft and Fraud*

94. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual learns that their PII and PHI was compromised, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

95. Plaintiffs and Class members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach.

96. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[34]

97. These efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[35]

98. And for those Class members who experience actual identity theft and fraud, the GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[36]

---

[34] *See* GAO Report *supra* n.35.

[35] *See* Federal Trade Commission, Identity Theft.gov, https://www.identitytheft.gov/Steps (last visited Oct. 2, 2023).

[36] GAO Report *supra* n.35.

L. *Diminution of Value of PII and PHI*

99. PII is a valuable property right.[37] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts that include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

100. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[38]

101. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[39]

102. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[40]

103. Conversely, sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[41]

104. Paired with PHI, packages of information about a single person can fetch up to $1,200 to $1,300 each on the black market.[42] The FBI's Cyber Division indicates that criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card

---

[37] *See, e.g.*, Randall T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[38] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES, available at: https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Oct. 2, 2023)

[39] *See*, e.g., https://datacoup.com/;

[40] Nielsen Computer & Mobile Panel, Frequently Asked Questions, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Oct. 2, 2023).

[41] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Oct. 2, 2023).

[42] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

number.[43]

105. As a result of the Data Breach, Plaintiffs' and Class members' PII and PHI, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class members for their property, resulting in an economic loss. Moreover, the PII and PHI is now readily available, and the rarity of the PII and PHI has been lost, thereby causing additional loss of value.

106. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII and PHI of Plaintiffs and Class members, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class members as a result of a breach.

107. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to, upon information and belief, millions of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

108. The injuries to Plaintiffs and Class members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII and PHI of Plaintiffs and Class members.

M. *Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary*

109. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII and PHI involved, the number of victims and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII and PHI for identity theft crimes ——e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or

[43] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

lines of credit; or file false unemployment claims.

110. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

111. Consequently, Plaintiffs and Class members are at a present and continuous risk of fraud and identity theft for many years into the future.

112. The retail cost of credit monitoring and identity theft monitoring can be around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class members from the risk of identity theft that arose from Defendants' Data Breach. This is a future cost that Plaintiffs and Class members would not need to bear but for Defendants' failure to safeguard their PII and PHI.

N. *Loss of the Benefit of the Bargain*

113. Furthermore, Defendants' poor data security deprived Plaintiffs and Class members of the benefit of their bargain. When agreeing to pay Defendants and/or its agents for products and/or services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the product and/or service and necessary data security to protect the PII and PHI, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiffs and Class members received products and/or services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants.

O. *Plaintiffs' Experiences*

114. Plaintiffs are both current patients within the CCH system, which is a part of Cook County. Cook County contracted with PJ&A for transcription and data storage services related to healthcare of the CCH and Cook County patients.

115. In order to obtain insurance and services through CCH and Cook County, Plaintiffs were required to provide their PII and PHI to Defendants, including their names, dates of birth, contact information, medical records, current health information, prescription records, and Social

Security numbers.

116. Upon information and belief, at the time of the Data Breach, Defendants retained Plaintiffs' PII and PHI in their systems.

117. On or about November 7, 2023 CCH sent notice by mail of the Data Breach event to Plaintiffs O'Neill and Moses.[44]

P. *Plaintiff O'Neill's Experience*

118. Plaintiff O'Neill is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII or PHI in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff O'Neill would not have entrusted her PII or PHI to Defendant had she known of Defendants' lax data security policies.

119. As a result of the Data Breach, and at the direction of Defendants' Notice, Plaintiff O'Neill made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

120. Plaintiff O'Neill suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

121. The Data Breach has caused Plaintiff O'Neill to suffer fear, anxiety, and stress,

[44] A copy of the notices sent to Plaintiffs are attached hereto as Exhibit A.

which has been compounded by the fact that Defendants have still not fully informed her of key details about the Data Breach's occurrence.

122. As a result of the Data Breach, Plaintiff O'Neill anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

123. As a result of the Data Breach, Plaintiff O'Neill is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

124. Plaintiff O'Neill has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Q. *Plaintiff Moses' Experience*

125. Plaintiff Moses is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII or PHI in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff Moses would not have entrusted his PII or PHI to Defendant had he known of Defendants' lax data security policies.

126. As a result of the Data Breach, and at the direction of Defendants' Notice, Plaintiff Moses made reasonable efforts to mitigate the impact of the Data Breach, including changing his passwords and monitoring his financial accounts for fraudulent activity. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

127. Plaintiff Moses suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII

and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII and PHI.

128. The Data Breach has caused Plaintiff Moses to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

129. As a result of the Data Breach, Plaintiff Moses anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

130. As a result of the Data Breach, Plaintiff Moses is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

131. Plaintiff Moses has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

132. Plaintiffs bring this action individually and on behalf of all others similarly situated pursuant to rules 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

133. Specifically, Plaintiffs propose the following class definition, subject to amendment as appropriate:

> All individuals in the United States whose PII/PHI was disclosed in the Data Breach (the "Class").

134. Plaintiffs also propose the following subclass definition, subject to amendment, as appropriate:

> All Illinois residents whose PII/PHI was disclosed in the Data Breach (the "Illinois Subclass")

135. The Class and the Illinois Subclass may be referred to collectively as the "Class."

136. Excluded from the Class are Defendants and its parents or subsidiaries, any entities

in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

137. Plaintiffs reserve the right to modify or amend the definition of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

138. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

139. Numerosity. The Class members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiffs believe that the proposed Class includes potentially millions of individuals who have been damaged by Defendants' conduct as alleged herein. The precise number of Class members is unknown to Plaintiffs but may be ascertained from Defendants' records. Current information indicates that 8,952,212 individuals were impacted and damaged by this Data Breach.[45]

140. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;

b. Whether Defendants' conduct violated the FTCA;

c. When Defendants learned of the Data Breach;

d. Whether Defendants' response to the Data Breach was adequate;

e. Whether Defendants unlawfully shared, lost, or disclosed Plaintiffs' and Class members' PII/PHI;

f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII/PHI compromised in the Data Breach;

g. Whether Defendants' data security systems prior to and during the Data Breach

[45] *See* U.S. Department of Health and Human Services Office for Civil Rights, Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, last accessed November 22, 2023.

complied with applicable data security laws and regulations;

h. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendants owed a duty to Class members to safeguard their PII/PHI;

j. Whether Defendants breached its duty to Class members to safeguard their PII/PHI;

k. Whether hackers obtained Class members' PII/PHI via the Data Breach;

l. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class members;

m. Whether Defendants breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class members;

n. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiffs and Class members suffered as a result of Defendants' misconduct;

p. Whether Defendants' conduct was negligent;

q. Whether Defendants was unjustly enriched;

r. Whether Plaintiffs and Class members are entitled to actual and/or statutory damages;

s. Whether Plaintiffs and Class members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

141. Typicality. Plaintiffs' claims are typical of those of other Class members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class members because, *inter alia*, all Class members were injured through the common misconduct of Defendants. Plaintiffs are advancing

the same claims and legal theories on behalf of himself and all other Class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class members arise from the same operative facts and are based on the same legal theories.

142. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

143. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class members in that all of Plaintiffs' and Class members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

144. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

145. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

146. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class members affected by the Data Breach.

COUNT I
NEGLIGENCE AND NEGLIGENCE *PER SE*
(By Plaintiffs Individually and on Behalf of the Class)

147. Plaintiffs incorporate by reference all previous allegations in paragraphs 1 through 146 as though fully set forth herein.

148. Defendants require their consumers, including Plaintiffs and Class members, to submit non-public PII and PHI in the ordinary course of providing their services.

149. Defendants gathered and stored the PII and PHI of Plaintiffs and Class members as part of its business of soliciting its services to its consumers, which solicitations and services affect commerce.

150. Plaintiffs and Class members entrusted Defendants with their PII and PHI with the understanding that Defendants would safeguard their information.

151. Defendants had full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiffs and Class members could and would suffer if the PII and PHI were wrongfully disclosed.

152. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

153. Defendants had a duty to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

154. Defendants owed a duty of care to Plaintiffs and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the

PII and PHI.

155. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and Class members. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential PII/PHI, a necessary part of being patients and consumers of Defendants services.

156. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII and PHI.

157. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Class.

158. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former consumers' PII and PHI it was no longer required to retain pursuant to regulations.

159. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

160. Defendants had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiffs and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

161. Defendants breached their duties, pursuant to the FTCA and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class members' PII and PHI. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' PII and PHI;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class members' PII and PHI;

d. Failing to detect in a timely manner that Class members' PII and PHI had been

compromised;

e. Failing to remove former consumers' PII and PHI it was no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

162. Defendants violated Section 5 of the FTCA by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class. Plaintiffs and Class members were within the class of persons the FTCA was intended to protect and the type of harm that resulted from the Data Breach was the type of harm it was intended to guard against.

163. Defendants' violation of Section 5 of the FTCA constitutes negligence per se.

164. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

165. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

166. It was foreseeable that Defendants' failure to use reasonable measures to protect Plaintiffs and the Class members' PII would result in injury to Plaintiffs and Class members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the entertainment industry.

167. Defendants have full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiffs and the Class could and would suffer if the PII/PHI were wrongfully disclosed.

168. Plaintiffs and the Class were the foreseeable and probable victims of any

inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII/PHI of Plaintiffs and the Class, the critical importance of providing adequate security of that PII/PHI, and the necessity for encrypting PII/PHI stored on Defendants' systems.

169. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs and Class members' PII/PHI would result in one or more types of injuries to Plaintiffs and Class members.

170. Plaintiffs and the Class had no ability to protect their PII/PHI that was in, and possibly remains in, Defendants' possession.

171. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

172. Defendants' duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

173. Defendants have admitted that the PII/PHI of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

174. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII/PIH of Plaintiffs and the Class would not have been compromised.

175. There is a close causal connection between Defendants' failure to implement security measures to protect the PII/PHI of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII/PHI of Plaintiffs and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII/PHI by adopting, implementing, and maintaining appropriate security measures.

176. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class

have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII/PHI; (iii) lost or diminished value of PII/PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII/PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII/PHI.

177. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

178. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII/PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII/PHI in its continued possession.

179. Plaintiffs and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

180. Defendants' negligent conduct is ongoing, in that Defendants still hold the PII/PHI of Plaintiffs and Class members in an unsafe and insecure manner.

181. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendants to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

COUNT II
BREACH OF IMPLIED CONTRACT
(By Plaintiffs Individually and on Behalf of the Class)

182. Plaintiffs incorporate by reference all previous allegations in paragraphs 1 through

146 as though fully set forth herein.

183. Plaintiffs and Class members were required to provide their PII and PHI to Defendants as a condition of receiving healthcare services from Defendants.

184. Plaintiffs and the Class entrusted their PII and PHI to Defendants. In so doing, Plaintiffs and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

185. In entering into such implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

186. Implicit in the agreement between Plaintiffs and Class members and the Defendants to provide PII/PHI, was the latter's obligation to: (a) use such PII/PHI for business purposes only, (b) take reasonable steps to safeguard that PII/PHI, (c) prevent unauthorized disclosures of the PII/PHI, (d) provide Plaintiffs and Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII/PHI, (e) reasonably safeguard and protect the PII/PHI of Plaintiffs and Class members from unauthorized disclosure or uses, (f) retain the PII/PHI only under conditions that kept such information secure and confidential.

187. The mutual understanding and intent of Plaintiffs and Class members on the one hand, and Defendants, on the other, is demonstrated by their conduct and course of dealing.

188. Defendants solicited, offered, and invited Plaintiffs and Class members to provide their PII and PHI as part of Defendants' regular business practices. Plaintiffs and Class members accepted Defendants' offers and provided their PII and PHI to Defendants.

189. In accepting the PII and PHI of Plaintiffs and Class members, Defendants understood and agreed that it was required to reasonably safeguard the PII and PHI from unauthorized access or disclosure.

190. On information and belief, at all relevant times Defendants promulgated, adopted, and implemented written privacy policies whereby they expressly promised Plaintiffs and Class

members that they would only disclose PII and PHI under certain circumstances, none of which relate to the Data Breach.

191. On information and belief, Defendants further promised to comply with industry standards and to make sure that Plaintiffs' and Class members' PII and PHI would remain protected.

192. Plaintiffs and Class members paid money and provided their PII and PHI to Defendants with the reasonable belief and expectation that Defendants would use part of its earnings to obtain adequate data security. Defendants failed to do so.

193. Plaintiffs and Class members would not have entrusted their PII and PHI to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure.

194. Plaintiffs and Class members would not have entrusted their PII and PHI to Defendants in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

195. Plaintiffs and Class members fully and adequately performed their obligations under the implied contracts with Defendants.

196. Defendants breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

197. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiffs and Class members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

198. Plaintiffs and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

199. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide

adequate credit monitoring to all Class members.

COUNT III
INVASION OF PRIVACY
(By Plaintiffs Individually and on Behalf of the Class)

200. Plaintiffs incorporate by reference all previous allegations in paragraphs 1 through 146 as though fully set forth herein.

201. Plaintiffs and Class members had a reasonable expectation of privacy in the PII and PHI Defendants mishandled.

202. As a result of Defendants' conduct, publicity was given to Plaintiffs' and Class members' PII and PHI, which necessarily includes matters concerning their private life.

203. A reasonable person of ordinary sensibilities would consider the publication of Plaintiffs' and Class members' PII and PHI to be highly offensive.

204. Plaintiffs' and Class members' PII and PHI is not of legitimate public concern and should remain private.

205. As a direct and proximate result of Defendants' public disclosure of private facts, Plaintiffs and Class members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) diminution of value of their PII/PHI; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their PII/PHI, which remains in Defendants' possession, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' PII/PHI.

206. Plaintiffs and Class members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

207. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii)

submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT IV
Unjust Enrichment
(By Plaintiffs Individually and on Behalf of the Class)

208. Plaintiffs incorporate by reference all previous allegations in paragraphs 1 through 146 as though fully set forth herein.

209. This count is pleaded in the alternative to the Breach of Implied Contract claim above (Count II).

210. Plaintiffs and Class members conferred a monetary benefit on Defendants. Specifically, they paid for services from and enrolled health care plans and services with Defendants and in so doing also provided Defendants with their PII and PHI. In exchange, Plaintiffs and Class members should have received from Defendants the services that were the subject of the transaction and should have had their PII and PHI protected with adequate data security.

211. Defendants knew that Plaintiffs and Class members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII and PHI entrusted to it. Defendants profited from Plaintiffs' retained data and used Plaintiffs' and Class members' PII and PHI for business purposes.

212. Defendants failed to secure Plaintiffs' and Class members' PII/PHI and, therefore, did not fully compensate Plaintiffs or Class members for the value that their PII/PHI provided.

213. Defendants acquired the PII and PHI through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

214. If Plaintiffs and Class members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII and PHI, they would not have entrusted their PII/PHI to Defendants or obtained health services as a patient from Defendants.

215. Plaintiffs and Class members have no adequate remedy at law.

216. Under the circumstances, it would be unjust for Defendants to be permitted to

retain any of the benefits that Plaintiffs and Class members conferred upon it.

217. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of PII/PHI; (iii) lost or diminished value of PII/PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII/PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII/PHI.

218. Plaintiffs and Class members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class members may seek restitution or compensation.

219. Plaintiffs and Class members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
(VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT ("ICFA"), 815 ILCS 505/1, *ET SEQ.*
(By Plaintiffs Individually as to Defendant PJ&A and on Behalf of the Illinois Subclass)

220. Plaintiffs incorporate by reference all previous allegations in paragraphs 1 through 146 as though fully set forth herein.

221. Plaintiffs are "consumers" as that term is defined in 815 ILCS 505/1(e).

222. Defendant PJ&A is engaged in "trade" or "commerce," including the provision of services, as those terms are defined under 815 ILCS 5051(f).

223. Defendant PJ&A engages in the "sale" of services as defined in 815 ILCS 505/1(b).

224. Defendant PJ&A engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts in connection with the sale and advertisement of "merchandise" (as defined in the ICFA) in violation of the ICFA, including but not limited to the following:

a. Failing to maintain sufficient security to keep Plaintiffs' and Illinois Subclass members' PII/PHI from being hacked and stolen; and

b. Failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and Illinois Subclass members' PII/PHI and other personal information from further unauthorized disclosure, release, data breaches, and theft.

225. In addition, Defendant PJ&A's failure to disclose that its computer systems were not well-protected and that Plaintiffs' and Illinois Subclass Members' PII/PHI was vulnerable and susceptible to intrusion and cyberattacks constitutes deceptive and/or unfair acts or practices because Defendant PJ&A knew such facts would (a) be unknown to and not easily discoverable by Plaintiff and Class Members; and (b) defeat Plaintiffs' and Illinois Subclass members' ordinary, foreseeable and reasonable expectations concerning the security of their PII/PHI on Defendant PJ&A's servers.

226. Defendant PJ&A intended that Plaintiffs and Illinois Subclass members rely on its deceptive and unfair acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts, in connection with its offering of services and incorporating Plaintiffs' and Illinois Subclass members' PII/PHI on its servers, in violation of the ICFA.

227. Defendant PJ&A also engaged in unfair acts and practices by failing to maintain the privacy and security of Plaintiffs' and Illinois Subclass members' PII/PHI, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45) and similar state laws.

228. Defendant PJ&A's wrongful acts and practices occurred within the ordinary course of trade or commerce.

229. Defendant PJ&A's wrongful acts and practices were and are injurious to the public interest because those practices were part of a generalized course of conduct on the part of Defendant PJ&A that applied to Plaintiffs and Illinois Subclass members and were repeated continuously before and after Defendant PJ&A obtained PII/PHI and other information from Plaintiffs and Illinois Subclass members. Plaintiff and Illinois Subclass members were adversely affected by Defendant PJ&A's conduct and the public was and is at risk as a result thereof.

230. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiffs and Illinois Subclass members of the nature and extent of the Data Breach pursuant to the Illinois Personal Information Protection Act, 815 ILCS 530/45, *et. seq*., which provides:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

231. 815 ILCS 530/20 provides that a violation of 815 ILCS 530/10 "constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act."

232. As a result of Defendant PJ&A's wrongful conduct, Plaintiffs and Illinois Subclass members were injured in that they never would have allowed their PII/PHI – the value over which Plaintiffs and Illinois Subclass members no longer have control – to be provided to Defendant PJ&A if they had been told or knew that Defendant PJ&A failed to maintain sufficient security to keep such data from being hacked and taken by others.

233. Defendant PJ&A's unfair and/or deceptive conduct proximately caused Plaintiffs' and Illinois Subclass members' injuries because, had Defendant PJ&A maintained customer PII/PHI with adequate security, Plaintiffs and Illinois Subclass members would not have lost it.

234. As a direct and proximate result of Defendant's conduct, Plaintiffs and Illinois Subclass members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made from Defendant that Plaintiffs and Illinois Subclass members would have never made had they known of Defendant PJ&A's careless approach to cybersecurity; lost control over the value of PII/PHI; harm resulting from damaged

credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII/PHI, entitling them to damages in an amount to be proven at trial.

235. Pursuant to 815 ILCS 505/10a(a), Plaintiffs and Illinois Subclass members seek actual and compensatory damages, injunctive relief, and court costs and reasonable attorneys' fees as a result of Defendant's violations of the ICFA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class members, request judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiffs and Plaintiffs' counsel to represent such Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII/PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class members;

iv. requiring Defendants to implement and maintain a comprehensive

Information Security Program designed to protect the confidentiality and integrity of the PII and PHI of Plaintiffs and Class members;

v. prohibiting Defendants from maintaining the PII and PHI of Plaintiffs and Class members on a cloud-based database;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel

how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third- party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, statutory, punitive, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand this matter be tried before a jury.

DATED: November 28, 2023

Respectfully Submitted,

STRANCH , JENNINGS & GARVEY, PLLC
/s/ Nathan R. Ring
NATHAN R. RING
Nevada State Bar No. 12078
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
Telephone: (725) 235-9750
lasvegas@stranchlaw.com

CARL V. MALMSTROM
(pro hac vice forthcoming)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, IL 60604
Telephone: (312) 984-0000
Facsimile: (212) 686-0114
malmstrom@whafh.com

RACHELE R. BYRD
(*pro hac vice forthcoming*)
ALEX J. TRAMONTANO
(*pro hac vice forthcoming*)
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com
tramontano@whafh.com

Attorneys for Plaintiffs and the Proposed Class

30187v3